FÓRMULA PARA OBTENER NÚMEROS DE CARMICHAEL CON n FACTORES PRIMOS, DONDE n ≥ 3.

Un entero positivo n es un número de Carmichael si ocurre que n es un número compuesto libre de cuadrados y cumple la congruencia lineal $a^{n-1} \equiv 1$ (mod. n) para todo natural a que sea primo relativo con n. Por ejemplo 561, 1105 y 1729 son los tres menores números de Carmichael.

A estos números se les denomina números de Carmichael en honor a Robert D. Carmichael (matemático norteamericano) quien los descubrió por primera vez en 1910; y en 1994 Alford, Granville, y Pomerance demostraron que existen infinitos números de Carmichael.

A los números de Carmichael también se les conoce como números pseudoprimos absolutos, el término pseudoprimo es debido a que 'se hacen pasar' como si fueran números primos al verificar un teorema que lo cumplen todos los números primos sin excepción. Este teorema es el pequeño teorema de Fermat: Si p es primo y a es un entero ≥ 2 tal que m.c.d (a, p) = 1 entonces se cumple que $\boldsymbol{a^{p-1}} \equiv 1$ (mod. p); y el término absoluto es debido a que esta congruencia se cumple para cualquier base a que sea primo relativo con el módulo p.

Con relación a los números primos, Dirichlet demostró que las sucesiones de la forma $\boldsymbol{a\,n + b}$ contiene infinitos números primos (con a y b coprimos positivos y con n que recorre todos los enteros no negativos).

Para los números de Carmichael ocurre algo similar, puesto que existen sistemas de sucesiones que contienen infinitos números de Carmichael. Estos sistemas de sucesiones son de la forma:

$$\begin{cases} Q_1(n) = (A^2\,B\,C)\,n + (A\,k + 1) \\ Q_2(n) = (A\,B^2\,C)\,n + (B\,k + 1) \\ Q_3(n) = (A\,B\,C^2)\,n + (C\,k + 1) \end{cases}$$

con tres factores primos, y de la forma:

$$\begin{cases} Q_1(n) = (A^2\,B\,C)\,n + (A\,k + 1) \\ Q_2(n) = (A\,B^2\,C)\,n + (B\,k + 1) \\ Q_3(n) = (A\,B\,C^2)\,n + (C\,k + 1) \\ Q_4(n) = (A^2\,B^2\,C^2)\,n + (A\,B\,C\,k + 1) \end{cases}$$

con cuatro factores primos, donde A ,B y C son números enteros positivos primos entre sí dos a dos y k es la solución principal ($0 \leq k < ABC$) de la congruencia lineal $(AB + AC + BC)\ X \equiv -(A + B + C) \pmod{ABC}$. Ambos sistemas producen números de Carmichael si para un mismo $\boldsymbol{n}$ entero no negativo se tiene que los $Q_i(n)$ son primos, en tal caso $Q_1(n)\ X\ Q_2(n)\ X\ Q_3(n)$ o $Q_1(n)\ X\ Q_2(n)\ X\ Q_3(n)\ X\ Q_4(n)$ es un número de Carmichael.

El producto de tres o más primos diferentes es un número de Carmichael, si cada primo disminuido en una unidad divide al producto (de dichos primos) disminuido también en una unidad; esta condición se conoce como el criterio de Korselt's.

Los números de Carmichael tienen como mínimo tres factores primos diferentes y como máximo no tienen límite. Esta afirmación se sustenta en los siguientes dos teoremas descubiertos y demostrados por el autor de este artículo:

TEOREMA

Sean:

$S = \prod_{i=1}^{n} \boldsymbol{p_i}$ un número de Carmichael.

m = M.C.M. (p_i - 1), $\forall$ i = 1, 2, 3, … , n.

D = { $\boldsymbol{d} \in \mathbb{N}$ / d es un divisor de $\frac{S-1}{m}$ }.

Si $\boldsymbol{md + 1}$ es primo diferente de $\boldsymbol{p_i}$, $\forall$ i = 1, 2, 3, … , $\boldsymbol{n}$; entonces $\boldsymbol{S(md + 1)}$ es un número de Carmichael.

Demostración.

Según Korselt's, para que $\boldsymbol{S(md + 1)}$ sea un número de Carmichael, éste debe cumplir con la siguiente condición:

M.C.M. [$(p_1 - 1)$; $(p_2 - 1)$; $(p_3 - 1)$; . . . ; $(p_n - 1)$; ((md + 1) – 1)] debe dividir a $S(md + 1) - 1$

Simplificando se tiene:

M.C.M. { M.C.M. [$(p_1 - 1)$; ($p_2 - 1$); ($p_3 - 1$); . . . ; ($p_n - 1$)], md } | [$Smd + S$ - 1]

M.C.M. $\{m\ ;\ md\}$ | [$Smd + S$ - 1]

md | ($Smd + S - 1$) (Observación: la expresión $a \mid b$ significa que a divide a b)

Luego, como $md \mid Smd$, entonces solo falta demostrar que $md \mid (S\text{-}1)$, es decir $\frac{s-1}{md} \in \mathbb{N}$; en efecto, puesto que: $\frac{s-1}{md} = \frac{\frac{s-1}{m}}{d}$; entonces $\frac{s-1}{md} \in \mathbb{N}$ porque, por hipótesis, d es un divisor de $\frac{s-1}{m}$. Luego, concluimos que $md \mid (Smd + S - 1)$.

POR LO TANTO $S(md + 1)$ ES NÚMERO DE CARMICHAEL.

---------- ■ ----------

Ejemplo. A partir del número de Carmichael **47006785** se pueden generar muchos más, tal como se muestra a continuación:

S_1 = 5 x 7 x 17 x 199 x 397 = 47006785	
S_1 x 3169 =	**148964501665**
S_1 x 6337 =	**297881996545**
S_1 x 19009 =	**893551976065**
S_2 = 148964501665	
S_2 x 34849 =	**5191263918523585**
S_2 x 4425697 =	**659271748125285505**
S_2 x 39026593 =	**5813576977927777345**
S_2 x 139610593 =	**20797022413400137345**
S_3 = 297881996545	
S_3 x 10631089 =	**3166810016767587505**
S_3 x 355044097 =	**1057612444758766448 65**
S_4 = 5191263918523585	
S_4 x 69697 =	**361815521329338303745**

S_4 x 209089 =	**1085436181460177864065**
S_4 x 409882177 =	**212780655630599764564464 5**
S_5 = 361815521329338303745	
S_5 x 139393 =	**5043455096466045417392678 5**
S_5 x 2648449 =	**958249955649164701215141505**
S_5 x 5296987 =	**191649954948280807309197926 5**
S_5 x 69068737 =	**249901410852139576853895200 65**
S_5 x 138137473 =	**499802818086123940414407363 85**
S_6 = 1085436181460177864065	
S_6 x 418177 =	**453904446054472798661109505**
S_7 = 453904446054472798661109505	
S_7 x 1254529 =	**569436290804271705631523046198145**
S_8 = 5043455096466045417392678 5	
S_8 x 418177 =	**210905692187488147450901811709 45**
S_8 x 20769409 =	**104749581671637751886404253372006 5**
S_9 = 569436290804271705631523046198145	
S_9 x 1544323969 =	**879394112707491082595273322219689646837505**
S_{10} = 210905692187488147450901811709 45	

S_{10} x 1254529 =	**26485730711427731813343239894204459905**
S_{10} x 19236097 =	**40570023527706641907158499875187160166 5**

Nota: los dos siguientes números de Carmichael:

2183111168989791463524609077490053772445543320990921477053678844729430358400000 1 (con 80 cifras**)** y

1733270528896519501068038107683055766943225204244446398152657471752662521561749850498099200001 = 41 x 61 x 101 x 601 x 1201 x 4801 x 14401 x 57601 x 172801 x 33696001 x 168480001 x 31505760001 x 441080640001 x 2205403200001 x 79394515200001 (con 94 cifras y quince factores primos), se los ha obtenido aplicando consecutivamente el teorema anterior.

Observación: no se sabe si a partir de un número de Carmichael se puede generar infinitos números de Carmichael.

Mediante este teorema se puede obtener números de Carmichael cada vez más grandes y con mayor cantidad de factores primos, pero el siguiente teorema muestra que existen números de Carmichael con la cantidad de factores primos que uno quiera (mil, un millón, un billón, …):

TEOREMA

Para todo $w \varepsilon \mathbb{N}$, con $w \geq 4$, sean Q_1(x), Q_2(x), … ,Q_n(x) sucesiones o funciones naturales de variable natural definidas por:

Q_1(x) = X + 1
Q_2(x) = 2 X + 1
Q_3(x) = 3 X + 1

Q_w(x) = 2^{w-3}(3) X + 1, donde w = 4, 5, 6, 7, …, z.

Si para un mismo X entero positivo ocurre que cada Q_j(x) es primo para j = 1, 2, 3, … w; entonces $\prod_{j=1}^{w}[Q_j(x)]$ es un número de Carmichael.

Demostración.

La secuencia de los Q_j**(x)** es como se muestra a continuación:

Q_1(x) = X + 1
Q_2(x) = 2 X + 1

Q_3(x) = 3 X + 1
Q_4(x) = 6 X + 1
Q_5(x) = 12 X + 1
Q_6(x) = 24 X + 1
Q_7(x) = 48 X + 1
Q_8(x) = 96 X + 1
.
.
.

Q_w(x) = 2^{w-3} (3 X) + 1

Sabemos que un número de Carmichael está formado por lo menos por tres factores primos diferentes, entonces para todo $\forall\, j \geq 3$ ocurre que $\prod_{j=1}^{w} [\boldsymbol{Q_j}(\boldsymbol{x})]$ es un número de Carmichael si se cumple que m.c.m. [$\boldsymbol{Q_j}$(x) - 1] divide a la diferencia $\{\prod_{j=1}^{w} [\boldsymbol{Q_j}(\boldsymbol{x})]\} - 1$.

Hallando el mínimo común múltiplo:

Numero de factores (j)	Q_j(x)	Q_j(x) – 1	Mínimo común múltiplo	Comentario
1	**= X + 1**	X		
2	**= 2 X + 1**	2 X		
3	**= 3 X + 1**	3 X	M.C.M. [X, 2 X, 3 X] = X [1, 2, 3] = 6 X	El m.c.m. para los tres primeros Q_j(x) – 1 es **6X.**
4	**= 6 X + 1** = 2^1 (3 X) + 1	6 X	M.C.M.[X, 2 X, 3 X,6X] = [[X, 2 X, 3 X],6X] = [6X, 6X] = 6 X	El m.c.m. para los cuatro primeros Q_j(x) – 1 es **6X.** (el último Q_j(x)-1)
5	**= 12 X + 1** = 2^2 (3 X) + 1	12 X	M.C.M. [6X, 12 X] = 12 X	El m.c.m. para los cinco primeros Q_j(x) – 1 es **12X.** (el último Q_j(x)-1)

6	$\mathbf{=24X+1}$ $=2^3(3X)+1$	$24X$	M.C.M. $[12X, 24X]$ $=24X$	El m.c.m. para los seis primeros $Q_j(x) - 1$ es **24X.** (el último $Q_j(x)$-1)
. . .	. . .	. . .	. . .	. . .
W	$\mathbf{=2^{w-3}(3X)+1}$	$2^{w-3}(3X)$	$2^{w-3}(3X)$	El m.c.m. para los $Q_j(x) - 1$ desde j = 1 hasta j = w es **2^{w-3} (3 X).** (el último $Q_j(x)$-1)

Para hallar el producto hacemos uso del resultado de un lema que no se incluye aquí por ser muy extenso. Este lema indica que $(A_1 X + 1)(A_2 X + 1)(A_3 X + 1)$ **. . .** $(A_h X + 1)$, es decir el producto de factores de la forma $A_i X + 1$ con i = 2, 3, 4, … h, es igual a

$$\{\sum [\prod (\boldsymbol{C}_h^h A_i)]\} X^h + \{\sum [\prod (\boldsymbol{C}_{h-1}^h A_i)]\} X^{h-1} + \{\sum [\prod (\boldsymbol{C}_{h-2}^h A_i)]\} X^{h-2} + \mathbf{\ldots} + \{\sum [\prod (\boldsymbol{C}_3^h A_i)]\} X^3 + \{\sum [\prod (\boldsymbol{C}_2^h A_i)]\} X^2 + \{\sum [\prod (\boldsymbol{C}_1^h A_i)]\} X + 1.$$

donde $\sum [\prod (\boldsymbol{C}_h^h A_i)]$ significa la sumatoria de los productos de todas las combinaciones de los A_i tomados de h en h; de igual manera, $\sum [\prod (\boldsymbol{C}_3^h A_i)]$ significa la sumatoria de los productos de todas las combinaciones de los A_i tomados de 3 en 3.

Ahora, para no dificultar la lectura (y más que nada, la escritura) vamos a convenir que el producto de los A_i; es decir $A_1 A_2 A_3 \ldots A_{h-3} A_{h-2} A_{h-1} A_h$ se escribirá simplemente como 1234…(h-3)(h-2)(h-1)(h); así, el producto $A_2 A_3 A_4 A_7 A_8 A_{10} A_{16}$ se representará solamente por 23478(10)(16); además, a la unidad se le representara por ***1***, en cursiva y en negrita.

Dicho esto, se tiene que el producto de los $\boldsymbol{Q_j(x)}$ esta distribuido, según el grado, en la siguiente tabla:

Términos de $\prod_{j=1}^{w} [Q_j(x)]$ (agrupados según el grado)	Grado	Significado	Simbólicamente
1234…(w-3)(w-2)(w-1)(w)	X^w	Sumatoria de los productos de todas las combinaciones de los A_w tomados de w en w	$\sum[\prod(C_w^w A_w)]$
1234…(w-4)(w-3)(w-2)(w-1) + 1234…(w-4)(w-3)(w-2)(w) + 1234…(w-4)(w-3)(w-1)(w) + 1234…(w-4)(w-2)(w-1)(w) . . . + 1245…(w-3)(w-2)(w-1)(w) + 1345…(w-3)(w-2)(w-1)(w) + 2345…(w-3)(w-2)(w-1)(w)	X^{w-1}	Sumatoria de los productos de todas las combinaciones de los A_w tomados de w-1 en w-1.	$\sum[\prod(C_{w-1}^w A_w)]$
12345…(w-5)(w-4)(w-3)(w-2) + 12345…(w-5)(w-4)(w-3)(w-1) + 12345…(w-5)(w-4)(w-2)(w-1) + 12345…(w-5)(w-3)(w-2)(w-1) . . . + 2356…(w-5)(w-4)(w-3)(w-2)(w-1)(w) + 2456…(w-5)(w-4)(w-3)(w-2)(w-1)(w) + 3456…(w-5)(w-4)(w-3)(w-2)(w-1)(w)	X^{w-2}	Sumatoria de los productos de todas las combinaciones de los A_w tomados de w-2 en w-2.	$\sum[\prod(C_{w-2}^w A_w)]$
. . .	. . .	. . .	. . .
123 + 124 + 125 + 126 . . . + (w-3)(w-2)(w-1) + (w-3)(w-2)(w) + (w-2)(w-1)(w)	X^3	Sumatoria de los productos de todas las combinaciones de los A_w tomados de 3 en 3.	$\sum[\prod(C_3^w A_w)]$

+ 12 + 13 + 14 + 15 . . . + (w-2)(w-1) + (w-2)(w) + (w-1)(w)	X^2	Sumatoria de los productos de todas las combinaciones de los A_w tomados de 2 en 2.	$\sum[\prod(C_2^w A_w)]$
1 + 2 + 3 + 4 + 5 . . . + (w-2) + (w-1) + (w)	X	Sumatoria de los productos de todas las combinaciones de los A_W tomados de 1 en 1.	$\sum[\prod(C_1^w A_w)]$
1		Termino independiente	

Ahora, $\forall\ \boldsymbol{w} \geq 4$ analizaremos la divisibilidad

m.c.m. [$[\boldsymbol{Q_1}(x)-1;\ [\boldsymbol{Q_2}(x)-1;\ \ldots\ [\boldsymbol{Q_j}(x)-1;]$ | $\{\prod_{j=1}^{w}[\boldsymbol{Q_j}(\boldsymbol{x})]-1\}$ .....(θ)

porque para $\boldsymbol{w} = 3$ ya se lo ha demostrado anteriormente (http://upload.wikimedia.org/wikipedia/commons/7/7a/Numeros_de_Carmichael.pdf)

Analizar la divisibilidad (θ) significa encontrar algún valor de $\boldsymbol{x}$ que permita que ésta se cumpla $\forall\ \boldsymbol{w} \geq 4$ (es decir para $\boldsymbol{w} = 4$, $\boldsymbol{w} = 5$, $\boldsymbol{w} = 6$,..., etc). Aunque ocurre que el divisor (el mínimo común múltiplo de los $\boldsymbol{Q_j}(x) - 1$) siempre es de primer grado, no sucede lo mismo con el dividendo o producto de los $\boldsymbol{Q_j}(x)$, pues cambia crecientemente de grado: cuando j = 4 el producto de los $\boldsymbol{Q_j}(x)$ es un polinomio de cuarto grado; si j = 5, el producto es un polinomio de quinto grado; para j = 6, es de sexto grado, y así sucesivamente.

Además el m.c.m. $[Q_1(x) - 1), Q_2(x) - 1), Q_3(x) - 1),\ldots,Q_w(x) - 1] = 2^{w-3}(3X)$

$\forall\, w \geq 4$, pero el producto $Q_1(x)\ Q_2(x)\ Q_3(x) \ldots Q_w(x)$ es un polinomio completo y ordenado de grado w que al restarle una unidad se queda sin término independiente; entonces es posible simplificar una X del divisor y del dividendo, y luego solo queda por encontrar algún valor para X tal que 3 (2^{w-3}) divida a:

$$\{ \sum [\prod (\boldsymbol{C}_w^w A_w)] \} X^{w-1} + \{ \sum [\prod (\boldsymbol{C}_{w-1}^w A_w)] \} X^{w-2} + \{ \sum [\prod (\boldsymbol{C}_{w-2}^w A_w)] \} X^{w-3} + \ldots + \{ \sum [\prod (\boldsymbol{C}_3^w A_w)] \} X^2 + \{ \sum [\prod (\boldsymbol{C}_2^w A_w)] \} X + \sum [\prod (\boldsymbol{C}_1^w A_w)]$$

Ésta es una tarea **muy, pero muy difícil**; pero teniendo presente que para $w \geq 4$ ocurre que el término independiente $\sum [\prod (\boldsymbol{C}_1^w A_w)]$ es igual al doble del mínimo común múltiplo, tal como se muestra a continuación:

$$\sum [\prod (\boldsymbol{C}_1^w A_w)] = X + 2X + 3X + 6X + 12X + \ldots + 2^{w-3} (3X)$$

$$= X + 2X + [\, 3X + 6X + 12X + \ldots + 2^{w-3} (3X) \,]^{o}$$

$$= X + 2X + 3X [1 + 2 + 4 + \ldots + 2^{w-3}]$$

$$= 3X + 3X \left[\frac{2^{w-2} - 1}{2 - 1} \right]$$

$$= 3X + 3X (2^{w-2} - 1)$$

$$= 3X (1 + 2^{w-2} - 1)$$

$$= 3X (2^{w-2})$$

$$= 2 [2^{w-3} (3X)]$$

$$= 2 \{ \text{m.c.m.} [\boldsymbol{Q_1}(x) - 1); \boldsymbol{Q_2}(x) - 1); \boldsymbol{Q_3}(x) - 1); \ldots; \boldsymbol{Q_w}(x) - 1] \} \quad \forall\, w \geq 4$$

entonces ahora la tarea resulta ser **muy fácil y sencilla**; para ello hacemos que m.c.m. $[\boldsymbol{Q_j}(x) - 1] = \boldsymbol{m}$ y en consecuencia $\sum [\prod (\boldsymbol{C}_1^w A_w)] = 2 [2^{w-3} (3)] = 2\boldsymbol{m}$; además si reescribimos al dividendo en una forma más sencilla, simplemente reemplazando los coeficientes que acompañan a las X por C_{w-1}, C_{w-2}, C_{w-3}, …,C_3, C_2, y C_1; tal como se muestra a continuación:

$$C_{w-1} X^{w-1} + C_{w-2} X^{w-2} + C_{w-3} X^{w-3} + \ldots + C_3 X^3 + C_2 X^2 + C_1 X + 2\,\boldsymbol{m}$$

entonces se tiene que la divisibilidad

$$\text{m.c.m.} [[\boldsymbol{Q_1}(x)\text{-}1;\ [\boldsymbol{Q_2}(x)\text{-}1; \ldots\ [\boldsymbol{Q_j}(x)\text{-}1;] \mid \{ \prod_{j=1}^{w} [\boldsymbol{Q_j}(\boldsymbol{x})] \text{-}1 \} \quad \ldots\ldots(\theta)$$

queda de la forma

$$\mathbf{m} \mid \{ C_{w-1} X^{w-1} + C_{w-2} X^{w-2} + C_{w-3} X^{w-3} + \ldots + C_3 X^3 + C_2 X^2 + C_1 X + 2\,\mathbf{m} \}$$

en donde se observa que ésta se cumple para X = **m** y en general se cumple cuando X = **m**n, con n **ε** $\mathbb{N}_0$, (es decir: X es múltiplo de **m**, incluido el cero, donde $\boldsymbol{m}$ **=** 3 [2^{w-3}]).

Por lo tanto; si para un mismo X = mn, con n ε $\mathbb{N}_0$, ocurre que cada uno de los Q_j (x) es primo, es decir para todo j = 1, 2, …, w, con w ≥ 4, **entonces** $\prod_{j=1}^{w} [Q_j (x)]$ **es un número de Carmichael.**

---------- ■ ----------

Nota: los dos teoremas de este artículo forman parte del libro **"Númerosde Carmichael"** elaborado por Juan Humberto Quiroz Mendoza (**juan109376@gmail.com**) y muy pronto estará disponible en forma gratuita a través de la web.